

Remarks and Arguments

Further to the Office Action mailed January 12, 2005, Applicant respectfully submits this amendment and requests reconsideration.

Rejections Under 35 U.S.C. §103

Claims 1-3, 5-7, 9-11 and 13-15 stand rejected under §103(a) as being unpatentable over Carlsson, U.S. Patent 6,490,367 in view of Lettvin, U.S. Patent 5,826,012. Applicant respectfully submits the following in traversal of this rejection.

In general, the present invention is directed to providing a certification authority for generating certificates in response to certification requests. Advantageously, as disclosed in the present specification, the certification authority generally includes a general purpose computer that is bootable from removable medium. The removable medium has encoded thereon an operating system module to boot the computer from the removable medium, in order to install an operating system, and a certificate generation module to control the computer to operate as the certification authority.

Advantageously, by placing the operating system module and the certificate generation module on the removable medium, a relatively inexpensive certification authority arrangement is provided. The expense of having to secure a system within, for example, a physically locked room, is reduced as only the removable medium need be secured. As Applicant points out, the resources necessary to secure a removable medium are much less than those necessary to secure a system in a dedicated room.

The Examiner maintains that the combination of Carlsson in view of Lettvin renders that which is claimed as being unpatentable. Applicant respectfully disagrees.

Carlsson is directed to a system for administering certificates and involves the generation, distribution and recall of certificates for public key systems (Abstract). Carlsson describes a system that requires a large amount of physical security in order to protect the certification authority from being compromised, much as was described by Applicant in the present specification. Particularly, Carlsson describes a system, with reference to Fig. 3, as having a CA terminal 6 in communication with a CA center. Further, as described by Carlsson, the CA terminal, while it may be placed in a physically unprotected environment (See Column 14, lines 46-47), must, nonetheless,

have strong physical protection. (See Column 14, lines 47-48). Protection must be provided so that unauthorized persons will not be able to "open" the terminal in order to exchange components, alter functions, copy information, etc. (Column 14, lines 48-50). Thus, as the Examiner has acknowledged, Carlsson does not disclose a computer that is bootable from a removable medium.

Independent claim 1, as amended, is directed to a certification authority for generating certificates where the certification authority comprises a general purpose computer that is bootable from a removable medium and a removable medium comprising a machine readable medium. Further, the machine readable medium has encoded thereon: an operating system module configured to enable the computer to boot an operating system from the removable medium and a certificate generation module configured to, after the computer has been booted, initiate a certificate generation session and control the computer to facilitate the generation of at least one certificate, as the certification authority, in response to an associated certification request. Further, upon booting from the removable medium, the computer is dedicated as a certification authority during the generation session and executes only operations related to the certificate generation session and, further, wherein remote control of the computer is prevented while the computer is dedicated as the certification authority.

The Examiner maintains that Lettvin teaches the use of a boot disk with additional applications stored thereon and that it would be obvious to combine the certificate generation hardware of Carlsson with the ability to boot from a removable medium with additional programs as taught by Lettvin in case the fixed medium fails.

Applicant respectfully submits that Lettvin does not remedy the deficiencies of Carlsson. Lettvin is directed to a computer storage medium that includes software that is executed at a startup of the computer prior to the computer executing an ultimate operating system. (Abstract) Lettvin describes hiding partitions on the disk in order to place a special start-up program which causes the computer to execute a boot-strap time operating system (BTOS) that, in turn, causes the computer to execute one or more programs, for example, an anti-virus program, disk-maintenance program and/or other programs stored in the hidden partition. (Column 4, lines 45-63; and Column 8, lines 23-32). Lettvin is silent as to a removable medium, let alone a medium, as

claimed in Applicant's claim 1, where a certificate generation module that causes the computer to operate as a certification authority is provided.

Applicant submits that the combination of Carlsson and Lettvin results in a certificate authority system that, in addition to the physical security of the CA center and the CA terminal, also includes the "hidden" BTOS program function that provides an additional level of security against an attack from "within", for example, viruses.

In contrast, claim 1 is directed to a certification authority comprising a general-purpose computer and the removable medium to cause the general purpose computer to operate as a certification authority. For at least the foregoing reasons, Applicant respectfully submits that the cited combination does not render obvious that which is recited in claim 1.

As claims 2, 3 and 5-7 depend from independent claim 1, Applicant respectfully submits that these claims are also not rendered obvious by the combination of Carlsson in view of Lettvin.

Independent claim 9, as amended, is directed to a computer program product for use in connection with a general purpose computer comprising of a removable medium having encoded thereon: an operating system module configured to enable the computer to boot an operating system from the removable medium and a certificate generation module. Similar to that which is recited in claim 1, the certificate generation module causes the computer to initiate a certificate generation session as the certification authority and dedicates the computer as the certification authority during a certificate generation session, executes only operations related to the certificate generation session and prevents remote control of the computer.

For at least the same reasons as submitted above with respect to independent claim 1, Applicant submits that independent claim 9, as amended, is not rendered obvious by the combination of Carlsson in view of Lettvin. Further, as claims 10, 11 and 13-15 depend from independent claim 9, Applicant submits that these claims are also not rendered obvious.

Claims 4 and 12 stand rejected under §103(a) as being unpatentable over Carlsson in view of Chaum, U.S. Patent 4, 529,870. Applicant respectfully traverses as follows.

Claims 4 and 12 depend from independent claims 1 and 9, respectively. Applicant submits that Chaum does not render the deficiencies of Carlsson with respect to either of independent claims 1 or 9.

Chaum is directed to a cryptographic apparatus that may be "personalized" to its owner. (Abstract). Chaum provides for a portable device for allowing an owner to identify himself to an external system where such identification is cryptographically secured. (Column 1, lines 10-13). Chaum, however, is silent as to providing certificate authority functionality by a removable medium.

The combination of Carlsson in view of Chaum results in the CA terminal and CA center described by Carlsson as having one more level of security provided by the cryptographically secured identification product of Chaum. This combination, however, does not obviate that which is recited in either of claims 1 or 9.

For at least the foregoing reasons, Applicant respectfully submits that dependent claims 4 and 12 are not rendered obvious by the cited combination of Carlsson in view of Chaum.

Claims 8 and 16 stand rejected under §103(a) as being unpatentable over Carlsson in view of Richard, U.S. Patent 5,922,074. Applicant respectfully traverses.

Dependent claims 8 and 16 depend from independent claims 1 and 9, respectively. Applicant submits that Richard does not remedy the deficiencies of Carlsson as submitted above with respect to the independent claims.

Similar to the purposes of Chaum, Richard provides for another level of security in being able to securely identify and authenticate a user. Richard, however, does not teach a removable medium to provide a general purpose computer with the functionality of a certification authority as recited in either of independent claims 1 and 9. For at least the foregoing reasons, Applicant submits that dependent claims 8 and 16 are not rendered obvious by the cited combination of Carlsson in view of Richard.

The amendments to the claims, as set forth herein, including the addition or cancellation of any claims, have been offered to advance this application to issue. None of the amendments made herein should be construed as an admission that the subject matter of the claims, as originally filed, is anticipated by or made obvious in light of any art of record whether considered singularly or in combination. Applicant